DMS 2.2 Gold *X.509 Certificate/FORTEZZA Card Reference Guide*

Sample X.509 Certificate Request Form

This *Reference Guide* provides information on how to request X.509 certificates and/or update your Fortezza card. X.509 certificates contain electronic security keys that enable you to sign and encrypt organizational messages. Each certificate is identified by a serial number. Certificate information, including your public encryption and/or signature key, is stored on the DMS Global Directory and on your Fortezza card. Your Fortezza card also provides you with authorized access to DMS organizational messaging.

There are two types of X.509 certificates – Version 1 (V1) and Version 3 (V3). V1 certificates support limited security clearances (Top Secret, Secret, Confidential, Sensitive But Unclassified, and Unclassified). V3 certificates provide additional levels of clearance, including NATO and Foreign clearances.

DMS 2.1 and 2.2 only support V1 certificates. V3 certificates will not be supported by DMS until Release 3.0 is implemented. Accordingly, this *Reference Guide* will only provide information on how to obtain, update, and delete V1 certificates.

What To Do First

- You may not know some of the information you are required to obtain. If you require assistance, consult your organization's system administrator, your Registration Authority (RA), or your Certification Authority (CA). These people can usually be contacted through your organization's Help Desk.
- Determine what you need. If you already have a Fortezza card, you will either require a new certificate or you will have to modify or delete existing certificates stored on the card. If you do not have a Fortezza card, you will need both a certificate and a Fortezza card.
- Prior to requesting an X.509 certificate, it is recommended that you obtain an e-mail address, including a distinguished name (DN), and that your address entry be stored in your organization's directory. Consult your organization’s system administrator or contact your Help Desk for more information.

Some Useful Definitions

Distinguished Names – DMS uses a messaging protocol called X.400 and a directory standard called X.500. Every directory entry receives an X.400 O/R address and an X.500 Distinguished Name (DN). Prior to requesting an X.509 certificate, it is recommended that you obtain an X.400 O/R address and an X.500 DN, and that your address entry be stored in your organization’s directory.

Individual Mail versus Organizational Mail – Individual mail is mail addressed to a specific person (e.g. John Smith). Organizational mail is mail addressed to a specific organization or role within an organization (e.g., Commander, USSTRATCOM) or the organization itself. Organizational mail will continue to be delivered regardless of who is assigned to read it. Access to both individual and organizational mail is granted via approved authorization within your organization.

Organizational or Official Name – When using organizational mail, your X.400 address will be an official, or organizational name, as opposed to your personal name. Check with your RA if you do not know your organizational name.

Personality – A personality is an ID stored on your Fortezza card. Fortezza cards can have multiple personalities, depending on the needs of the user. Each personality has its own X.509 certificates and each Fortezza card has its own PIN (or password) to grant access.

Completing the X.509 Certificate Request Form

The National Security Agency (NSA) X.509 Certificate Request Form is used to request X.509 certificates and Fortezza cards, or to make changes to existing certificates or cards. You can obtain a copy of the form on the DISA DMS Home Page at http://www.disa.mil/D2/dms. Navy personnel can obtain a copy of the form from the NCTC web site at http://www.nctcdms.navy.mil. A login ID and password are required. Once at the site, go to Customer Support / DMS Forms / X.509 Certificate.
Upon completion, send this form to your Supervisor for signature approval. Your Supervisor will approve the request and forward it to your organization’s Security Officer. The Security Officer must verify the clearances and security categories selected and sign the form. The Security Officer will then forward the request to the CA or RA for action. It normally takes about one week to process a certificate or Fortezza card request. Your Supervisor or your organization’s Help Desk or RA may be able to provide you with more specific information.

The X.509 Certificate Request form is divided into three pages:

- Page 1 is used to identify the request being made, the individual making the request and provide background information and administrative information needed to fulfill the request.
- Page 2 is used to provide information about X.509 V3 certificates. *Do not use this page for DMS certificates until DMS 3.0 is implemented.*
- Page 3 is used to provide information about X.509 V1 certificates.

This *Reference Guide* will provide guidance for completing pages 1 and 3 of the X.509 Certificate Request Form. V3 certificates are not addressed in this *Reference Guide*.

PAGE 1 – GENERAL INFORMATION

Block 1 – Request Type

The Request Type box identifies the specific activity you need performed relating to your X.509 certificate. Requests are grouped into three basic categories – new certificate requests, change requests, and performing selected administrative tasks concerning either your certificate or your Fortezza card.

The following tables display the request type, discuss when you would select the request type, and document the remaining block numbers on the form that will require information.

New Requests

Prior to requesting an X.509 certificate, it is recommended that you obtain an e-mail address, and a distinguished name (DN), and that your address entry be stored in your organization's directory. Consult your organization's system administrator or contact your Help Desk for more information.

Request Type (Block 1):	When to select this Request Type:	X.509 Certificate Request Form Block Numbers You Must Complete:
• New Certificate	• You do not currently have a Fortezza card • You require an additional certificate for your Fortezza card *Note: Each certificate request must be made on a separate form.*	2-6, 7 (if you already have a card), 7b (if requesting a new card), 9, 10, 11 (if necessary), 13-15. Requests for V1 certificates must also complete blocks 32-36 on page 3 of the X.509 Certificate Request Form.

Change Requests

Request Type (Block 1):	When to select this Request Type:	X.509 Certificate Request Form Block Numbers You Must Complete:
Update Certificate	• If you need to modify clearance levels for a certificate • If you wish to extend the validity period for your certificate or keys. • If your information stayed the same but the directory your certificate is stored in has changed. • If any other attribute for your certificate changes.	2, 6-8, 10 (if the host name of the directory in which your certificate is to be posted has changed), 13-15. For a V1 certificate, specify any modifications in blocks 32-36 on page 3 of the X.509 Certificate Request Form.
Change User Information	• If you need to modify information about yourself (e.g., phone number change) • If the address where you want your Fortezza card mailed has changed. • If the address where you want your PIN sent has changed • If your e-mail address has changed. *Note: You only need to submit page 1 of the X.509 request form.*	Enter *updated information only* in blocks 2-5. Enter original certificate usage type in box 6. Enter *original* name and addresses in block 11. If the host name of the directory for one of your DNs has changed (in which that certificate is to be posted), enter the DN in block 9, and the *new* directory in block 10. You and your supervisor must fill out blocks 13 and 14 respectively.

Request Type (Block 1):	When to select this Request Type:	X.509 Certificate Request Form Block Numbers You Must Complete:
Change PIN	• If someone else discovered your PIN but you still retained possession of your Fortezza card. • If your unit's policy requires you to change your PIN on a periodic basis.	2, 3-4 (if changed), 7, 11 (explain why you want your PIN changed). You and your supervisor must fill out blocks 13 and 14 respectively.

Administrative Requests

Request Type (Block 1):	When to select this Request Type:	X.509 Certificate Request Form Block Numbers You Must Complete:
Reprint PIN	• If you forgot your PIN number.	2, 4, 7 You and your supervisor must fill out blocks 13 and 14 respectively.
Renew PIN	• If you want to reactivate certificate that has expired.	7-9, 11 You and your supervisor must fill out blocks 13 and 14 respectively.
Send Certificate	• If you want to send a copy of a certificate in binary format (a soft copy) to a specified location. The certificate (s) can be posted to a directory, copied to a diskette (in MS-DOS format), or sent through e-mail to another person.	2, 3, 5, 6, 8, 11 You and your supervisor must fill out blocks 13 and 14 respectively.
Copy Card	• If you want another copy of your Fortezza card for use at a separate site or for backup purposes.	2, 7, 11 You and your supervisor must fill out blocks 13 and 14 respectively.
Delete Certificate	• If you are no longer a government employee or if you change jobs and your new function no longer requires this certificate.	2, 7-8 You and your supervisor must fill out blocks 13 and 14 respectively.
Report Compromise	• If your Fortezza card was lost or stolen cards.	2-9, 11 You and your supervisor must fill out blocks 13 and 14 respectively. You must also attach a detailed report in accordance with policy NAG-69C paragraph 37.

The following pages describe the remaining information blocks on the X.509 Certificate Request form.

2 User's Full Name/Phone

Enter your full name. This can include: title, first name, middle name or initial, last name and suffix (e.g., Jr.). It is mandatory that at least the first name and last name be specified.

Enter the commercial and DSN (optional) telephone number(s) of the user.

3 Card Address

Enter the address where the user's hardware token (e.g., Fortezza card) should be shipped. This address must include a street address. *Do not use a P.O. box address.*

4 PIN Address

Enter the address where the user's PIN letter should be mailed. For a more secure distribution, the Fortezza card and PIN addresses should be different. It is recommended that user's home address be used for the PIN address. This field is optional if you will pick up the PIN letter personally from your CA or RA.

5 E-mail Address

Enter the e-mail address where you will receive official communications with the CA.

Some users, such as RAs, can support encrypted MMP messaging to the CA. For these special users, fill out the following information. If the address supports sequence signed MMP messages to the CA, check the box. If the address supports encrypted MMP messaging to the CA, select the "encryption enabled" box that indicates that encrypted messages are to be used when sending to that address. If encryption is enabled for the address, then it is necessary to specify which of the User's DNs to use. You must also specify the Universal parameters and security policy (e.g. GENSER). This allows the CAW to determine which certificate to use for the key exchange. Universal selection either comes from the superior authority's certificate or from the list of universals stored in the database. The universals in this encryption certificate request must match the universals in the CA's encryption certificate in order for the two to communicate. If there is a guard in the network that separates this user from the CA, you also need to specify that a guard token is necessary.

SUPPORTING INFORMATION

This section contains information used to uniquely identify the user, their certificate, and their card. It is also used to provide additional information relative to the request being made.

6 Certificate Usage

- *Individual*. You will be using your certificate(s) for individual purposes rather than for organizational messaging communication.
- *Organizational*. You will be using your certificate(s) on behalf of an organization. The "firstborn" certificate is the first to be requested on behalf of a specific organization and is posted to the organization's directory entry. The actual Fortezza card typically not issued to a user. Subsequent requests should be marked as "siblings". The organizational firstborn certificate contains an encryption key that will be shared by the siblings. Sibling certificates are used for organizational messaging, but are not necessarily posted to the directory since the sibling DN's do not need to be stored in the directory.

  Specify whether this is a firstborn or a sibling organizational certificate. You will also be required to identify the official name of the organizational messaging group.

  For sibling certificates, select the appropriate privilege in block 36. (Note: You must follow local procedures for authorizing organizational certificates.)

7 Card Chip Serial Number

This field is only filled out when you already have a Fortezza card. Enter the card chip serial number, which is found on the card label.

7b. Card Clearance

Use this field when you are requesting a Fortezza card. Check the box that supports the highest classification of certificate that will be placed on this card. For example if your card will contain unclassified certificates and a secret certificate, check the "Secret" box.

8 Certificate Identifier

Enter the Fortezza card slot of the certificate upon which the action should be taken. .

9 Distinguished Name (DN)

Prior to requesting an X.509 certificate, it is recommended that you obtain an X.400 O/R address and an X.500 distinguished name (DN), and that your address entry be stored in your organization's directory. Consult your organization's system administrator or contact your Help Desk for more information.

Enter your DN in this block. The DN should be entered here or attached to this form.

10 Directory

Enter the host name of the directory server to which your certificate will be posted/mastered. Consult your e-mail systems administrator if you require assistance.

11 Explanatory Information

Additional information or justification is **required** for the following actions:

- Change Card Point of Contact. Enter the original device or organizational card user's name, phone number(s), address, and e-mail address.
- Change PIN. Enter which PIN is to change: SSO or User. Normally this would be User.
- Change User Information. Enter your original information.
- Copy Card. Indicate the reason for the copy card request (e.g., traveling user, card to be used outside of a classified enclave, or device requires multiple cards). If the same PIN is required, state so here.
- New certificate.
  - If multiple cards are needed containing the requested certificate, indicate the quantity of cards and the reason (e.g., traveling user, card to be used outside of a classified enclave, or device requires multiple cards).
  - For sibling organizational certificate requests, enter the user name (organization) of the owner of the organizational firstborn certificate.
  - If the certificate or certification path is needed on floppy disk, state which and enter the desired filename.
  - If the user needs a certificate from a different CA loaded on an existing card, indicate the justification for placing the certificate on this card (e.g. temporary assignment in region different from normal CA).
- Rekey. Indicate which key (signature, encryption, or both) must be rekeyed.
- Report Compromise. A compromised certificate can result in an unauthorized user sending organizational mail under your name.

Your certificate has been compromised if anyone other than yourself has had access to your Fortezza card and its PIN. Compromises usually occur if you have lost your Fortezza card or have logged on with your Fortezza card and PIN and you have left your workstation unattended.

Enter the serial number(s) of the certificate(s) whose key has been compromised and the reason for compromise, including the scope of the compromise (e.g., all certificates on card, all certificates issued to user). Indicate the date of the suspected compromise. Attach additional pages if necessary.

- Restore. Indicate why the card or certificate(s) needs to be restored and the scope of the restore (e.g., entire card or single certificate).
- Send Certificate. State the following:
  - ⇒ What media is required (e.g., MS-DOS diskette, MMP message, DAT tape, etc.).
  - ⇒ The destination of the certificate (i.e., DSA, another CAW).

ADMINISTRATIVE/SIGNATURE BLOCK

This section is for administrative information and the approval signatures. Blocks 12, 16, 17, and 18 should be completed by your RA or CA.

The authority must enter the type of identification that was used to verify the user's identity (e.g., driver's license, military ID).

13 User Signature
You must sign and date the completed form prior to submission.

This signature acknowledges your responsibilities to:

- accurately represent yourself in all communications with the PKI;
- protect your private keys at all times, in accordance with this policy, as stipulated in the certificate acceptance agreements and local procedures;
- Notify, in a timely manner, the organization that issued your certificates of suspicion that your private keys are compromised or lost.
- Abide by all the terms, conditions, and restrictions levied upon the use of your private keys and certificates.

14 Supervisor Name
Print the name of the supervisor who is approving the requested action. Enter the commercial and DSN (optional) telephone number(s) of the supervisor. Obtain the supervisor's signature when the form is ready for submission.

15 Security Officer Name
Print the name of the security officer who is approving the requested action. Enter the commercial and DSN (optional) telephone number(s) of the security officer. Obtain the security officer's signature when the form is ready for submission. Before signing, the security officer must verify the user is authorized for access to any clearances, privileges, and security categories requested on the form.

Page 2 - Version 3 Certificate Information – Blocks 16-31
DMS 2.1 and DMS 2.2 only support V1 certificates. DMS will not support V3 certificates until Release 3.0. *Do not enter any information on this page.*

Page 3 - Version 1 Certificate Information – Blocks 32-36
This section contains information specific to version 1 X.509 certificates.

32 Certificate Validity Period (V1)
If you are requesting a new v1 certificate this block must be completed. X.509 certificates are only valid for a specific period of time. The default validity varies by organization, but can be no greater than 3 years. You can elect one of the following options:

- A start date and time only – The certificate will be valid for the default time period beginning with this date/time.
- An end date and time only – The certificate will be valid from the date/time it is created until the end date/time specified.
- A start and end date and time – The certificate will be valid for the length of time specified.
- A start date and time and the period after that date (e.g., 3 months) – The certificate will be valid for the length of time specified beginning on the date/time recorded.
- A period only (e.g., 3 months) – The certificate will be valid for the period specified. The start date/time will be when the certificate is created.

Enter dates in the following format: MM/DD/YYYY HH:MM. Specify days, weeks, months, or years when entering a period.

33 Personality (V1)
If you are requesting a new version 1 certificate this block must be completed. Enter the name that will be used to identify the X.509 certificate on the hardware token (e.g., Fortezza card). If preferred, you can defer this to your CA. The Personality name must be unique for each certificate on a Fortezza card and in order to select the correct Fortezza role when messaging should be meaningful by including part of the DN, the maximum classification level (e.g. S for Secret), and certificate version (e.g. v1). This field has a maximum length of 24 characters.

34 KEA Clearances (V1)
If you are requesting a new version 1 certificate this block must be filled in. Select all classification levels to be supported by the requested X.509 certificate. The requested classifications cannot exceed the clearance level of the user.

35 KEA Privileges (V1)
If you are requesting a new version 1 certificate this block must be completed. Select the communication privileges that must be supported by this certificate. If you need more information, consult your CA.

36 DSS Privileges (V1)
This block is optional and need only be completed if you have specific signature privileges or limitations. Select all that apply.

The Following pages contain an example of a completed X.509 certificate

Sample X.509 Certificate Request Form

Page 1 of 2

User Information

1. Request Type
New Certificate

2. User's Full Name *(Print)*
John B. Centcomuser

Phone Comm. (123)456-7890
DSN 968-7890

3. Card Address *(See instructions if card is to be mailed)*
Org.
Street 1234 Main St.
City Linthicum
State/AA,AE,AP MD Postal Code 21090
Country US

4. PIN Address *(See instructions if card is to be mailed)*
Org.
Street 5678 First Street
City Linthicum
State/AA,AE,AP MD Postal Code 21090
Country US

5. E-mail Address
jbcentcomuser@centcom.mil

ONLY FOR MMP ENABLED APPLICATIONS

□ Sequence Signed?
□ Encryption Enabled?
□ Guard Token Necessary?

Security Policy (if encryption enabled)
□ GENSER
□ Other ________

Universal Selection (if encryption enabled)
□ Extract from Authority Certificate
□ Specify KEA Universals
Universal name:____________

Supporting Information

6. Certificate Usage *(See instructions for additional information required)*
☒ Individual □ Registration Authority
Organizational: □ Firstborn □ Sibling Org Name ____________
□ Device: Type ________________

7. Card Chip Serial Number
(For existing card only)
____

7b. Card Clearance
□ Top Secret ☒ Secret □ Confidential □ Unclassified

8. Certificate Identifier *(For existing certificate only, enter certificate serial number or see instructions)*
____

9. Distinguished Name *(See instructions for inclusion of blank spaces)*
C=US,o=O=U.S. Government,ou=DoD,ou=Centcom,cn=JBCentcomuser

10. Directory Name *(to which certificate is to be posted)*
CentcomSecretdir

11. Explanatory Information *(See instructions; continue on separate sheet if necessary)*
____

Administrative/Signature Block

12. Type of Identification

13. User Signature **Date**

14. Supervisor Name *(Print)* **Phone** Comm. (123)456-7891 **Signature** *(see instructions)* **Date**
Jane Smith DSN 968-7891

15. Security Officer Name *(Print)* **Phone** Comm. (123)456-7800 **Signature** *(see instructions)* **Date**
Lori L. Smith, LTC, USA DSN 968-7800

16. Registration Authority Name *(Print)* **Phone** Comm. ________ **Signature** **Date**
________________ DSN ________

17. Certification Authority Name *(Print)* **Phone** Comm. ________ ature Date
________________ DSN ________

18. Number of pages approved _______ *(Authority use only)*

Each signer of this form certifies that the statements or signatures made on this form are true, complete, and correct to the best of my knowledge. I understand that false statements are subject to civil and criminal penalties, including but not limited to penalties under 18 U.S.C. Section 1001.

Privacy Act Statement

Authority: GNSA15 (Computer Users Control System); P.L. 86-38; P.L. 88-290.

Principal Purpose: To collect relevant information to issue a X.509 certificate.

Routine Use(s): See Blanket Routine Uses at 58 Fed. Reg. 10531 (Feb. 22, 1993) and GNSA15.

Effect On Individual If Information Is Not Provided: May prevent processing of certificate application or result in denial of certificate.

Sample X.509 Certificate Request Form

Page 2 of 2

32. Certificate Validity Period (v1)

☒ Use default period

□ Specify period

Start ________________

End ________________ or Period _____________

33. Personality (v1) *(maximum length of 24 characters)*

CentcomuserDispatch___________

34. KEA Clearances (v1)
(Select all that apply)

□ Top Secret

☒ Secret

☒ Confidential

☒ Sensitive But Unclassified

☒ Unclassified

35. KEA Privileges (v1)
(Select all that apply)

☒ Critic/Flash

☒ Immediate/Priority

☒ Routine/Deferred

□ Multifunction Interpreter (MFI)

36. DSS Privileges (v1)
(Select all that apply)

□ Organizational Releaser

□ No Signature Capability/Read Only

Privacy Act Statement

Authority: GNSA15 (Computer Users Control System); P.L. 86-38; P.L. 88-290.

Principal Purpose: To collect relevant information to issue a X.509 certificate.

Routine Use(s): See Blanket Routine Uses at 58 Fed. Reg. 10531 (Feb. 22, 1993) and GNSA15.

Effect On Individual If Information Is Not Provided: May prevent processing of certificate application or result in denial of certificate.